

Search

 Entire Site

☒ All Books

☐ Current Book Only

 GO >

Advanced Search

Table of Contents



Book

**Cisco® Field
Manual: Router
Configuration**

Copyright

About the Authors

Acknowledgments

Introduction

► Configuration Fundamentals

► Layer 2 Networking

► Network Protocols

► Packet Processing

► Voice & Telephony

▼ Security

▼ Security and VPNs

Suggested Ways to
Secure a Router
**Authentication,
Authorization, and
Accounting (AAA)**
Dynamically
Authenticate and
Authorize Users with
Authentication ProxyControlling Access
with Lock and Key
SecurityFiltering IP Sessions
with Reflexive Access
ListsPrevent DoS Attacks
with TCP InterceptIntelligent Filtering
with Context-Based
Access Control
(CBAC)Detect Attacks and
Threats with the IOS
Intrusion Detection
SystemUsing Internet Key
Exchange (IKE) for
VPNs

IPSec VPN Tunnels

• Print • E-Mail This Page • Add Bookmark

Cisco® Field Manual: Router Configuration

Table of Contents • Index

- TEXT 200

Security and VPNs > Authentication, Authorization, and Accounting (AAA)

13-2. Authentication, Authorization, and Accounting (

- Method lists are used to specify a sequence of methods to use for each component. If a method receives no response or an error condition, the next method in the list is tried.
- Multiple AAA servers can be defined. If the first one listed doesn't respond or generates an error, the next server is tried.
- AAA servers can be grouped so that a collection of servers can be used for a specific purpose.
- Authentication can use a variety of methods, including RADIUS, TACACS+, Kerberos, and locally configured in the router.
- Authorization can use RADIUS and TACACS+ to authorize users to access available resources.
- Accounting can use RADIUS and TACACS+ to track and record the services and network resources that users are using.
- Shared secret keys are configured in both the router and the RADIUS or TACACS+ server. The shared secret key interaction (including the user's password entry) is encrypted.

Configuration

1. Enable AAA functionality:

```
(global) aaa new-model
```

2. Identify one or more AAA servers.

a. Use a RADIUS server.

- (Optional) Set global defaults for all RADIUS servers.

Set the shared router/server key:

```
(global) radius-server key {0 string | 7 string | string}
```

The shared secret encryption key is set as *string* (a cleartext string), or if the string appears by itself, the string appears unencrypted in the router configuration. If **7** precedes it, the string is "hidden" and encrypted in the configuration.

Further Reading

- ▶ Access Lists and Regular Expressions

- ▶ Appendixes
- Index

Browse by Category

- ▶ Applied Sciences
- ▶ Artificial Intelligence
- ▶ Business
- ▶ Certification
- ▶ Computer Science
- ▶ Databases
- ▶ Desktop Publishing
- ▶ Desktop Applications
- ▶ E-Business
- ▶ E-Commerce
- ▶ Enterprise Computing
- ▶ Graphics
- ▶ Human-Computer Interaction
- ▶ Hardware
- ▶ Internet/Online
- ▶ IT Management
- ▶ Markup Languages
- ▶ Multimedia
- ▶ Networking
- ▶ Operating Systems
- ▶ Programming
- ▶ Security
- ▶ Software Engineering

View All Titles >

Set the request timeout interval:

```
(global) radius-server timeout seconds
```

After a request, the router waits for *seconds* (1 to 1000; the default response from a RADIUS server).

Set the number of request retries:

```
(global) radius-server retransmit retries
```

If no response is received from a RADIUS server, the router retransmits *retries* times (1 to 100; the default is 3).

Set the server deadtime:

```
(global) radius-server deadtime minutes
```

If a RADIUS server doesn't respond after the retransmit retries, mark it as "dead" for a period of time in *minutes* (0 to 1440; the soon as it is marked as dead, the router skips that server and selects the next available server.

- Specify one or more servers to use:

```
(global) radius-server host {hostname | ip-address} [authentication-port port] [timeout seconds] [retransmit retries] [alias {hostname | ip-address}] [key string]
```

The RADIUS server is identified by host name or IP address. You specify the UDP ports for authentication (**auth-port**; the default is 1645) and accounting (**acct-port**; the default is 1646). You can override the defaults and set the number of seconds the router waits for a RADIUS response with **timeout** (1 to 1000) and set the number of retransmitted requests with **retransmit** (1 to 100). The **alias** keyword can be used to define up to eight host names or a single RADIUS server name. The shared secret **key** can be set to a string. Always set the key as the last argument so that any error message is not confused with other arguments.

- (Optional) Enable vendor-specific RADIUS attributes (VSAs):

```
(global) radius-server vsa send [accounting | authorization]
```

The router can recognize VSAs that comply with attribute 26 of the RADIUS protocol, either **accounting** or **authorization**.

- (Optional) Enable vendor-proprietary RADIUS attributes:

```
(global) radius-server host {hostname | ip-address} no ietf
```

The router can use IETF draft extensions for the most common vendor-specific attributes.

b. Use a TACACS+ server.

- (Optional) Set the global shared router/server key for TACACS+:

```
(global) tacacs-server key key
```

The shared secret encryption key is set as *string* (a cleartext string; spaces are accepted).

- Specify one or more servers to use:

```
(global) tacacs-server host hostname [port port] [time
string]
```

The TACACS+ server is identified by host name. You can specify with the **port** keyword (the default is 49). The amount of time the TACACS+ response is **timeout** in seconds. The shared secret **key** *string* (a cleartext string). Always set the key as the last argument; embedded spaces will not be confused with other arguments.

c. Use a Kerberos server.

- Create users and SRVTAB entries on the Key Distribution Center

Users and SRVTAB entries are administered on the Kerberos server. See the Kerberos documentation for further instructions. The SRVTAB file and associated keys will be imported into the router in a later step.

- Identify the Kerberos realm.

Define a default realm:

```
(global) kerberos local-realm realm
```

The router is located in the Kerberos *realm* (an uppercase text string). All resources are registered to a server. This should be taken from the *realm* parameter on the server.

Specify the Kerberos server for the realm:

```
(global) kerberos server realm {hostname | ip-address}
```

The server for the *realm* (an uppercase text string) is identified by the IP address and also by the *port* used for the KDC (the default is 88). The IP address or IP address should be taken from the *admin_server* parameter on the server itself.

(Optional) Map a DNS domain or host name to the realm:

```
(global) kerberos realm {domain | hostname} realm
```

A *domain* (a fully qualified domain name with a leading dot) or a *hostname* (a fully qualified host name with a leading dot) can be mapped to a specific *realm* (an uppercase text string).

- Import a SRVTAB file.

Create a DES encryption key:

```
(global) key config-key 1 string
```

A private DES key is created as key number **1** using *string* (up to 16 alphanumeric characters). The key is used to generate DES keys for SRVTAB entries.

TFTP the SRVTAB file and create SRVTAB entries:

```
(global) kerberos srvtab remote tftp://hostname/filename
```

The SRVTAB file is identified by its URL using the server's host name followed by the filename. The file is retrieved via TFTP.

d. (RADIUS or TACACS+ only) Group a list of servers.

- Define a group name:

```
(global) aaa group server {radius | tacacs+} group-name
```

A server group named *group-name* is created. The group can identify configured RADIUS or TACACS+ servers that can be used for a particular service.

- Add a server to the group:

```
(server-group) server ip-address [auth-port port] [acct-port port]
```

The server at the IP address is a member of the group. You can specify ports for authentication (**auth-port**; the default is 1645) and accounting (**acct-port**; the default is 1646).

- (Optional) Set a deadtime for the group:

```
(server-group) deadtime minutes
```

The group deadtime allows the router to skip over a group of servers that are unresponsive and declared "dead" and send requests to the next group. Deadtime is in *minutes* (0 to 1440; the default is 0).

3. Use AAA authentication.

a. Create a method list for an authentication type:

```
(global) aaa authentication {login | ppp | nas | arap | enable} list-name method1 [method2 ...]
```

The method list named *list-name* is created. It contains a list of login authentication methods to be tried in sequential order. The **default** keyword specifies a list of methods for the default authentication. The list can include the authentication type given by **login** (the login prompt on the router), the privileged EXEC command level, **ppp** (dialup access through PPP), **nas** (Network Access Server Asynchronous Services Interface), or **arap** (AppleTalk Remote Access Protocol).

The method keywords (*method1*, *method2*, ...) given in the list depend on the authentication type:

- **login—enable** (use the enable password), **krb5** (Kerberos 5), **krb4** (Kerberos 4 for Telnet authentication), **line** (use the line password), **local** (use

usernames and passwords), **local-case** (use the router's list of case-sensitive usernames), **none** (use no authentication; every user is successfully authenticated), **group radius** (use all listed RADIUS servers), **group tacacs+** (use all listed TACACS+ servers), and **group group-name** (use only the servers listed in the *group-name*).

- **enable— enable** (use the enable password), **line** (use the line password), **local** (use the router's list of case-sensitive usernames), **local-case** (use the router's list of case-sensitive usernames), **none** (use no authentication; every user is successfully authenticated), **group radius** (use all listed RADIUS servers), **group tacacs+** (use all listed TACACS+ servers), and **group group-name** (use only the servers listed in the server group named *group-name*).
- **ppp— if-needed** (no authentication if the user is already logged in (Kerberos 5)), **local** (use the router's list of case-sensitive usernames), **local-case** (use the router's list of case-sensitive usernames), **none** (use no authentication; every user is successfully authenticated), **group radius** (use all listed RADIUS servers), **group tacacs+** (use all listed TACACS+ servers), and **group group-name** (use only the servers listed in the server group named *group-name*).
- **nasl— enable** (use the enable password), **line** (use the line password), **local** (use the router's list of case-sensitive usernames), **local-case** (use the router's list of case-sensitive usernames), **none** (use no authentication; every user is successfully authenticated), **group radius** (use all listed RADIUS servers), **group tacacs+** (use all listed TACACS+ servers), and **group group-name** (use only the servers listed in the server group named *group-name*).
- **arap— auth-guest** (allow a guest login if the user has EXEC access), **line** (use the line password), **local** (use the router's list of case-sensitive usernames), **local-case** (use the router's list of case-sensitive usernames), **none** (use no authentication; every user is successfully authenticated), **group radius** (use all listed RADIUS servers), **group tacacs+** (use all listed TACACS+ servers), and **group group-name** (use only the servers listed in the *group-name*).

b. Apply the method list to a router line or interface.

- (PPP only) Authenticate on an interface.

Select an interface:

```
(global) interface type slot/number
```

Enable PPP authentication on the interface:

```
(interface) ppp authentication {protocol1 [protocol2 .  
[list-name | default] [callin] [one-time]
```

PPP authentication can be used with one or more protocols (*protocol1*): **chap** (CHAP), **ms-chap** (Microsoft CHAP), or **pap** (PAP). The **no** keyword prevents additional authentication if TACACS or extend already authenticated a user. The method list is specified as *list-name*, a list of methods that PPP sequentially tries. If a method list is not needed, the **default** keyword causes PPP to use the default method. The **callin** keyword causes PPP to use the default method. The **one-time** keyword causes PPP to use the default method. The **callin** keyword causes PPP to use the default method. The **one-time** keyword causes PPP to use the default method. The **callin** keyword causes PPP to use the default method. The **one-time** keyword causes PPP to use the default method.

- (Login, NASL, or ARAP only) Authenticate on a line.

Select a line:

```
(global) line {aux | console | tty | vty} line-number
```

A specific Aux, console, async, or virtual TTY line can be selected by *line-number*. Add the *end-line-number* to select a range of line numbers.

Apply authentication to the line:

```
(line) {login | nasi | arap} authentication {default |
```

The authentication type is given as **login**, **nasi**, or **arap**. The *method-list-name* is used to authenticate users on the line. The **default** keyword is used instead to use the default AAA authentication methods with the *method-list*.

c. (Optional) Use the AAA banners and prompts.

- Create a login banner:

```
(global) aaa authentication banner dstringd
```

The customized banner *string* (up to 2996 characters) is displayed before the username login prompt. The *d* character is a delimiter (any character that must appear before and after the banner string).

- Change the password prompt:

```
(global) aaa authentication password-prompt string
```

The default password prompt string is Password:. You can change the password prompt text string; enclose it in double quotes if it contains spaces).

- Create a failed login banner:

```
(global) aaa authentication fail-message dstringd
```

The customized banner *string* (up to 2996 characters) is displayed before the failed login prompt. The *d* character is a delimiter (any character that doesn't appear before and after the banner string).

4. Use AAA authorization.

a. Create a method list for an authorization type:

```
(global) aaa authorization {auth-proxy | network | exec | config-  
reverse-access | configuration | ipmobile} {default | list-name [method1 [method2 ...]]
```

The method list named *list-name* is created. It contains a list of authorization methods to be tried in sequential order. The **default** keyword specifies a list of methods and interfaces that are configured for default authorization. The list of methods is given by **auth-proxy** (use specific policies per user), **network** (related service requests), **exec** (permission to run a router EXEC), **config** (use all commands at privilege level, 0 to 15), **reverse-access** (permission to use Telnet connections), **configuration** (permission to enter router configuration mode), and **ipmobile** (permission to use IP mobility).

The method keywords (*method1*, *method2*, ...) given in the list are **group** (requests to the servers in the group named *group-name*), **group radius** (requests to the RADIUS server group), **group tacacs+** (send requests to the TACACS+ server group).

authenticated (permission is granted if the user is already authenticated authorization; every user is successfully authorized), and **local** (use the r usernames and passwords).

b. Apply the method list to a line or an interface.

- Authorize users on a line.

Select a line:

```
(global) line line-number [end-line-number]
```

An Aux, console, async, or virtual TTY line can be selected with t Add the *end-line-number* to select a range of line numbers.

Apply authorization to the line:

```
(line) authorization {arap | commands level | exec | r  
[default | list-name]
```

The authorization type is given as **arap** (AppleTalk Remote Acce **commands** *level* (permission to execute commands at privilege (permission to use a router EXEC shell), or **reverse-access** (pe reverse Telnet). The method list named *list-name* is used to autl line. The **default** keyword can be used instead to use the default methods without specifying a method list.

- (PPP only) Authorize users on an interface.

Select an interface:

```
(global) interface type slot/number
```

Apply authorization to the interface:

```
(interface) ppp authorization [default | list-name]
```

The method list named *list-name* is used to authorize PPP users The **default** keyword can be used instead to use the default AA/ methods without specifying a method list.

5. Use AAA accounting (RADIUS or TACACS+ only).

a. Create a method list for an accounting type:

```
(global) aaa accounting {auth-proxy | system | network | ex  
connection [h323] | commands level} [default | list-name]  
stop-only | wait-start | none} [broadcast] group {radius  
group-name}
```

The method list named *list-name* is created. It contains the accounting m The **default** keyword specifies a method to be used on lines and interface for default accounting. The accounting type records information about **aut** events), **system** (system-level events), **network** (network-related servic (router EXEC sessions), **connection** (outbound connections from an acce/ performs H.323 gateway accounting for Voice over IP), and **commands** (privilege *level*, 0 to 15.

The method used for accounting can be **group** *group-name* (send records group named *group-name*), **group radius** (send records to the RADIUS server group), or **group tacacs+** (send records to the TACACS+ server group).

The **broadcast** keyword causes records to be sent to multiple accounting servers. Accounting records are selected by **start-stop** ("start" when a process begins; "stop" when the process ends), **stop-only** (no "start" is sent; "stop" when the process ends), **start-only** ("start" when a process begins; the process doesn't actually begin until "stop" is sent to the server; "stop" when the process ends), or **none** (no accounting is performed).

b. (Optional) Record accounting for failed authentications:

```
(global) aaa accounting send stop-request authentication failure
```

The router sends "stop" records when a user authentication or a PPP negotiation fails.

c. Apply the method list to a line or an interface.

- Perform accounting on a line.

Select a line:

```
(global) line line-number [end-line-number]
```

An Aux, console, async, or virtual TTY line can be selected with the `line` command. Add the *end-line-number* to select a range of line numbers.

Enable accounting on the line:

```
(line) accounting {arap | commands level | connection
[default | list-name]}
```

The accounting type is given as **arap** (AppleTalk Remote Access), **commands level** (EXEC commands at privilege *level*), **connect** (connection authentication), or **exec** (router EXEC shell). The method list name is the method list used for accounting on the line. The **default** keyword can be used to use the default AAA accounting method without specifying a method.

- (PPP only) Perform accounting on an interface.

Select an interface:

```
(global) interface type slot/number
```

Enable accounting on the interface:

```
(interface) ppp accounting default
```

The default method is used for PPP accounting on the interface.

Example

The router is configured for AAA using all three authentication, authorization, and accounting methods. RADIUS servers are identified as 192.168.161.45 and 192.168.150.91, both having the TACACS+ server is at 192.168.44.10. One local username is also defined. It is used as the event that the AAA servers are inaccessible.

Authentication is set up for PPP access on async interfaces using the RADIUS servers, for authentication. Authentication is also used for login access to the router via Telnet, using the RADIUS servers, and then local authentication.

Authorization is configured to use the RADIUS servers and local authentication for both functions. Users entering the network via PPP and Telnet must be authorized. Accounting is configured on the RADIUS servers for both network and exec resource reporting. The router sends accounting data for both PPP and router exec terminal sessions.

```

aaa new-model
radius-server host 192.168.161.45 key aAaUsInGrAdIuS
radius-server host 192.168.150.91 key aAaUsInGrAdIuS
tacacs-server host 192.168.44.10 key tacacs-server-1

aaa authentication login router-login group tacacs group radius local
aaa authentication ppp ppp-login group radius local
aaa authorization network default group radius local
aaa authorization exec default group radius local
aaa accounting network default start-stop group radius
aaa accounting exec default start-stop group radius

username admin password letmein

interface async 1
 encapsulation ppp
 ppp authentication pap ppp-login
 ppp authorization default
 ppp accounting default

line vty 0 4
 login authentication router-login
 authorization exec default
 accounting exec default

```

Cisco® Field Manual: Router Configuration

 Table of Contents • Index

 TEXTZOO

URL <http://proquest.safaribooksonline.com/1587050242/ch13lev1sec2>